

AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20)

☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

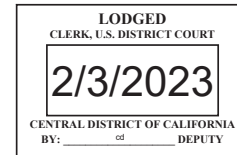
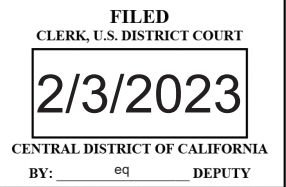
United States of America

v.

Cristian Chimirel and
Petrisor Orbuletu,

Defendant(s)

Case No. 2:23-mj-00521-DUTY



**CRIMINAL COMPLAINT BY TELEPHONE
OR OTHER RELIABLE ELECTRONIC MEANS**

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of February 2, 2023 in the county of Los Angeles in the Central District of California, the defendant(s) violated:

Code Section

18 U.S.C. § 1029(a)(2)

Offense Description

Use of unauthorized access devices

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/ Jacqueline Cenana, Special Agent

Complainant's signature

Jacqueline Cenana, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: February 3, 2023 at 2:00 p.m.



Judge's signature

City and state: Los Angeles, California

Maria A. Audero

Hon. ~~Karen Stevenson~~, U.S. Magistrate Judge

Printed name and title

AUSA: Nisha Chandran (x2429)

AFFIDAVIT

I, JACQUELINE CENAN, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against Cristian Chimirel ("CHIMIREL") and Petrisor Orbuletu ("ORBULETU") for a violation of 18 U.S.C. § 1029 (a) (2) (use of unauthorized access devices).

2. This affidavit is also made in support of an application for a warrant to search the following digital devices in the custody of the United States Secret Service ("USSS"), in Los Angeles, California, as described in Attachment A-1:

a. Silver Apple iPhone retrieved from CHIMIREL's person with a broken screen. USSS was unable to obtain the model or serial number of this iPhone as the phone was locked ("SUBJECT DEVICE 1");

b. Black Apple iPhone on ORBULETU's person. USSS was unable to obtain the model or serial number as the phone was locked ("SUBJECT DEVICE 2," and collectively with SUBJECT DEVICE 1, the "SUBJECT DEVICES").

3. This affidavit is also made in support of a search warrant for a 2022 silver Ford Explorer bearing California license plate 8ZPB602 and Vehicle Identification Number 1FMSK7DH6NGA52352 (the "SUBJECT VEHICLE") as described in Attachment A-2, confirmed by CHIMIREL to be rented by CHIMIREL.

4. The affidavit is also made in support of a search warrant for a storage unit previously rented by CHIMIREL and located at Public Storage, 20140 Sherman Way, Winnetka, California 91306, Unit 1213, as described in Attachment A-3.

5. The requested search warrants seek authorization to seize evidence, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 1028 (Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information), 1029 (Access Device Fraud), 1344 (Bank Fraud), and 1028A (Aggravated Identity Theft) (collectively, the "Subject Offenses"), as described more fully in Attachment B.

6. Attachments A-1, A-2, A-3, and B are incorporated herein by reference.

7. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and search warrants, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND OF AFFIANT

8. I am a Special Agent ("SA") with the United States Secret Service ("USSS") and have been so employed since March

2021. In this capacity, I am responsible for investigating violations of federal criminal laws relating to financial institution fraud, credit card fraud, bank fraud, cybercrimes, and identity theft. I am a graduate of the Criminal Investigator Training Program conducted at the Federal Law Enforcement Training Center in Glynco, Georgia, as well as the USSS Special Agent Training Course in Beltsville, Maryland. I have received advanced training in financial and cybercrime investigations including the Basic Investigation of Computers and Electronic Crimes Program, Basic Network Intrusion Responder Training, and I have received continued education related to the investigation and prosecution of cybercrimes. I have participated in multiple investigations in connection with fraud and cybercrimes.

III. SUMMARY OF PROBABLE CAUSE

9. Between August 2022 and January 2023, the California Department of Social Services has detected more than \$38.9 million in stolen funds from victim Electronic Benefit Transfer ("EBT") cards. Much of this fraud is from one specific program known as CalFresh, which helps low-income households purchase food and household items to meet their nutritional needs. Many of the fraudulent withdrawals are done at specific ATMs in the Central District of California.

10. For example, between on or about January 1, 2023, and on or about January 5th, 2023, more than approximately \$117,000 was withdrawn from ATMs at a single financial institution branch located in Toluca Lake, California in Los Angeles County. The

unauthorized withdrawals conducted during these five days and at this single bank branch affected approximately 152 victim EBT cardholders. The dates of these withdrawals coincided with the disbursement by DSS of CalFresh benefits to EBT cardholders.

11. Law enforcement has also reviewed ATM surveillance provided by financial institutions that administer EBT accounts that relate to the fraud scheme at issue. During the unauthorized ATM withdrawals, suspects can often be seen holding stacks of cards and conducting withdrawals in quick succession at one ATM.

12. On or about February 2, 2023, at approximately 4:45 a.m. (PST), law enforcement conducted physical surveillance at a U.S. Bank ATM terminal located at 19500 Ventura Boulevard, Tarzana, California, which was identified by law enforcement as one of the top 30 ATM U.S. Bank locations for CalFresh fraud. CHIMIREL and ORBULETU arrived in the SUBJECT VEHICLE and proceeded to the ATM terminal located at the US Bank branch where law enforcement was conducting surveillance. At the ATM, law enforcement observed, and U.S. Bank confirmed that, CHIMIREL withdraw cash from the ATM in rapid succession using approximately five different access devices. CHIMIREL handed the withdrawn cash, totaling \$7,240, to ORBULETU as CHIMIREL proceeded to use the next card. CHIMIREL and ORBULETU were arrested and found possessing the SUBJECT DEVICES. A card to a storage unit in CHIMIREL's name was found in CHIMIREL's wallet.

IV. STATEMENT OF PROBABLE CAUSE

13. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. Regulatory Background of CalFresh Program

14. The California Department of Social Services (hereinafter "DSS") is a government agency that administers several benefit and assistance programs for residents of the state of California. One of the assistance programs administered by DSS is called CalFresh (formerly known as food stamps), which helps low-income households purchase food and household items to meet their nutritional needs.

15. Residents of California that meet the criteria established by the CalFresh program can apply online for benefits at www.getcalfresh.org.

16. CalFresh benefits are issued through Electronic Benefit Transfer cards ("EBT cards"). EBT cards are mailed to an address designated by the account holder and function like traditional debit cards to conduct transactions. For example, you can use an EBT card to make a purchase at a grocery or convenient store by swiping the card at a point-of-sale terminal.

17. The EBT cards issued under this program are assigned specific Bank Identification Numbers ("BIN"). A BIN refers to the first five digits of the account number on a debit or credit card and can be used to identify the benefit program, like the CalFresh program, associated with the card.

18. Benefits received through the program are typically disbursed to EBT cardholders by DSS during the early days of each month. Those benefits are deposited directly from DSS into the account of the EBT cardholder. The CalFresh Program is for low-income individuals who meet certain federal income eligibility rules and want to add to their budget to purchase healthier food options. Beneficiaries apply for benefits by submitting their income and number of dependents to determine their benefit eligibility. Those benefits are distributed once a month, typically during the early days of each month.

19. The CalFresh Program allows EBT cardholders to conduct cash withdrawals at automated teller machines (ATMs) using a personal identification number (PIN) established by the cardholder. The EBT cardholder presents the card at an ATM, inserts the card into the ATM card reader, and utilizes a PIN to withdraw the funds previously deposited by the CalFresh Program

B. Background on CalFresh Fraud in Los Angeles Area and Prior Operation

20. Since in or about August 2022, local law enforcement has been working with DSS to investigate a significant increase in unauthorized cash withdrawals utilizing EBT cards. Based on analysis of victim complaints to DSS, victim complaints to local law enforcement, bank records, and surveillance, law enforcement determined that the majority of the unauthorized cash withdrawals were being conducted with cloned cards.

21. A cloned card can be a blank white plastic card or another debit, credit or gift card that contains altered

information on the card's magnetic stripe. Based on my training and experience, I know that suspects will often clone cards by taking stolen card information from a victim card's magnetic stripe and re-encode that stolen information onto another card's magnetic stripe. Cloning these cards allows the suspect to use the card and the DSS benefits added on to the account linked to the card for illicit purchases or unauthorized cash withdrawals.

22. On a legitimate debit or credit card, the information coded on the card's magnetic stripe will match the information embossed on the front of the card. This information includes the account number, expiration date, and cardholder's name, among other information. Whereas on a cloned card, the information coded on the magnetic stripe will not match the information embossed on the front of the card. For example, if a suspect re-encodes victim EBT card information onto a pre-existing gift card's magnetic stripe or a blank white plastic card with a magnetic stripe, the magnetic stripe will be coded with the EBT card information, but the card itself will still bear the information of the gift card or bear no information if it is a blank white plastic card.

23. Based on my training, experience, and participation in this investigation, I know that the victim card data harvested to clone cards is often obtained from what is colloquially referred to as "skimming activity."

24. The term "skimming" is used to describe activity that involves unlawfully obtaining debit and credit card information by using technological devices to surreptitiously record victim

accountholder's debit and credit card numbers and personal identification numbers at, for example, ATMs or point-of-sale terminals. For example, individuals conducting ATM "skimming" may install a skimming device into the card reader of the ATM to record the debit or credit card numbers, as well as a camera or keypad overlay on the ATM keypad to record the associated PIN number. Those individuals will then return to the ATM to collect the card number and PIN information stored on the installed device.

25. As described above, suspects then manufacture cloned and fraudulent debit or credit cards that bear the victim accountholder's account information that was obtained from skimming. Once that information is loaded onto another fraudulent card (e.g., a gift card or blank plastic card), members of the scheme then use that fraudulent card to withdraw cash from the victim accountholder's bank accounts or to make purchases with the victim accountholder's account.

26. In or about September 2022, local law enforcement conducted a surveillance and arrest operation in the Los Angeles, California area. This operation was planned in response to the large number of unauthorized withdrawals occurring at ATMs in the Los Angeles area during a short period of time. Specifically, law enforcement had analyzed fraudulent EBT withdrawal data and noticed a high volume of unauthorized withdrawals on specific dates and times that coincided with the dates when the majority of benefits are disbursed to EBT cardholders.

27. As a result of this operation, local law enforcement established surveillance at select Bank of America ATMs that were used to conduct a significant volume of CalFresh fraud. Law enforcement surveilled those ATMs around the dates when benefits had been disbursed, observed suspects that withdrew a high volume of unauthorized withdrawals and that conducted those withdrawals in rapid succession, and arrested multiple individuals believed to be making fraudulent withdrawals of CalFresh benefits. As a result, law enforcement arrested approximately 16 suspects. All of the arrested suspects were later determined to be citizens of countries other than the United States who did not have documentation to be lawfully present in the United States. All of the individuals arrested were released from local custody within hours of their arrest and absconded from any future judicial proceedings.

C. Background of Current Operation to Combat CalFresh Fraud

28. Data provided by DSS, based in part upon reported fraud by victims, reported fraud to local law enforcement, bank records, and surveillance indicates that as of in or about January 2023, there has been approximately \$71.3 million in stolen funds from victim EBT cards.

29. For the previous six months, between in or about August 2022 and in or about January 2023, in the Central District of California and elsewhere, more than approximately \$38.9 million has been stolen from victim EBT cards. The

majority of these stolen funds have been obtained by unauthorized ATM withdrawals.

30. In early January 2023, more than approximately \$7.2 million was stolen from victim EBT cards largely through unauthorized ATM withdrawals. Of the approximately \$7.2 million stolen from victim EBT cards in the beginning of January 2023, more than approximately \$2.9 million was stolen, almost entirely through unauthorized ATM withdrawals, in Los Angeles County alone.

31. For example, in early January 2023, more than approximately \$117,000 was withdrawn from ATMs at a single financial institution branch located in Toluca Lake, California in Los Angeles County. The unauthorized withdrawals conducted during these days and at this single bank branch affected approximately 152 victim EBT cardholders. The dates of these withdrawals coincided with the disbursement by DSS of CalFresh benefits to EBT cardholders.

32. Based upon my training and experience conducting access device fraud investigations, I know that suspects committing access device fraud schemes will often target particular BINs when harvesting stolen card information collected from skimming devices. Thus, suspects using skimming may target the BIN associated with CalFresh benefits. Moreover, based upon my training and experience, the sheer volume of unauthorized ATM withdrawals occurring during the early days of the month is further indicative that suspects participating in the fraud scheme at issue are targeting EBT cards because

benefits are typically disbursed to EBT cardholders during the early days of each month.

33. Law enforcement has also reviewed ATM surveillance provided by financial institutions that administer EBT accounts that relate to the fraud scheme at issue. During the unauthorized ATM withdrawals, suspects can often be seen holding stacks of cards and conducting withdrawals in quick succession at one ATM. Based upon my training and experience, I know that suspects perpetrating access device fraud schemes will often conduct unauthorized withdrawals using cloned cards in rapid succession at ATMs.

34. Based upon the rapid succession of unauthorized ATM withdrawals being conducted, the fact that the cards being used to conduct the unauthorized cash withdrawals are nearly all cloned EBT cards, and the fact that nearly all of the unauthorized withdrawals are happening during the early days of the month, I believe that suspects participating in the fraud scheme at issue are ostensibly targeting EBT cards.

D. CHIMIREL & ORBULETU Committed CalFresh Fraud Using Fraudulent Cards on February 2, 2023

35. Based upon the large dollar amount being stolen from victim EBT cards, the number of victims impacted, the concentration of unauthorized ATM withdrawals occurring in particular areas, and the large number of unauthorized ATM withdrawals occurring at singular bank locations, law enforcement decided to conduct a surveillance and arrest operation in February 2023.

36. On or about February 2, 2023, law enforcement was conducting physical surveillance at a U.S. Bank ATM terminal located at 19500 Ventura Boulevard in Tarzana, CA ("Tarzana ATM"), which was identified by U.S. bank as one of the top 30 U.S. Bank ATM locations in Los Angeles for CalFresh fraud. Based on the CalFresh fraud data, surveillance was conducted from approximately 4:45 a.m. to approximately 6:15 a.m.

37. On February 2, 2023, between 12:00 a.m. and 1:00 p.m., the total of all EBT card cash withdrawals made across 77 U.S. Bank ATM terminals in Los Angeles County was \$335,155 in cash withdrawals. In total, at those same 77 locations, \$417,020 in EBT card cash withdrawals was made between the hours of 12:00 a.m. to 3:00 a.m.¹

38. DSS reported to law enforcement that the CalFresh benefits had been disbursed into the EBT accounts at approximately 12:00 a.m. on February 2, 2023.

39. During this surveillance, law enforcement observed two unknown individuals, later identified as CHIMIREL and ORBULETU, arrive in the SUBJECT VEHICLE and approach the Tarzana ATM at approximately 6:00 a.m. Law enforcement observed CHIMIREL in the driver's seat of the SUBJECT VEHICLE and ORBULETO in the passenger's seat of the SUBJECT VEHICLE.

40. After CHIMIREL and ORBULETU exited the SUBJECT VEHICLE and approached the Tarzana ATM, law enforcement observed CHIMIREL conduct multiple transactions which appeared to be

¹ At those same locations between the hours of 1:00 a.m. to 2:00 a.m. \$76,910 were made in cash withdrawals. Between 2:00 a.m. to 3:00 a.m., \$4,955.

withdrawals based upon law enforcement observing CHIMIREL retrieve what appeared to be currency at the conclusion of each transaction and pass the currency back to ORBULETU, who was standing beside CHIMIREL at the Tarzana ATM terminal. CHIMIREL appeared to conduct several withdrawal transactions in rapid succession while law enforcement observed for approximately eight minutes. CHIMIREL appeared to insert several different cards to conduct withdrawals, and pass the retrieved currency and/or cards back to ORBULETU on multiple occasions. Based upon my training and experience, individuals conducting legitimate transactions at ATMs typically conduct a single transaction and do not transition between multiple payment cards rapidly to conduct several transactions in a short period of time.

41. While CHIMIREL and ORBULETU were at the Tarzana ATM, law enforcement learned from U.S. Bank that the first withdrawal transaction took place on an EBT account belonging to an individual named R.O. Law enforcement similarly confirmed with California's Department of Motor Vehicles ("DMV") that the individual conducting the ATM withdrawals did not appear to match R.O. CHIMIREL then made approximately four additional transactions on EBT accounts belonging to additional victims, totaling \$7,240.

42. Based on the date, time, ATM location, presence of multiple, and successive ATM withdrawals on multiple EBT cardholder accounts during a short time period, law enforcement detained CHIMIREL and ORBULETU in order to investigate further.

43. CHIMIREL had approximately 10 cloned EBT cards in his jacket and pant pockets. ORBULETU had approximately 5 cloned EBT cards in his jacket and pant pockets. The cloned cards consisted of a variety of re-encoded prepaid cards and gift cards. The cards also had stickers placed on them with, what appeared to be, based on my training and experience and later confirmed by CHIMIREL, card balances and victim PINs.

44. Law enforcement confirmed these were cloned EBT cards by reading the magnetic stripe and determined through United States Department of Agriculture Office of Inspector General that the cards belonged to other real individuals, not CHIMIREL or ORBULETU. Moreover, the cloned cards also were affixed with stickers bearing victim PIN numbers that corresponded to each cloned card and were needed in order to conduct the unauthorized ATM withdrawals.

45. ORBULETU also had approximately \$7,857 in cash in his jacket pockets, which was close in value to the approximately \$7,240 in total unauthorized ATM withdrawals. Tarzana ATM surveillance photographs obtained by law enforcement also clearly depicted CHIMIREL and ORBULETU at the ATM conducting the unauthorized withdrawals using cloned EBT cards and directly corroborated law enforcement's surveillance observations.

46. When asked to identify himself, CHIMIREL provided the name "Emil" and produced an identification card from Slovakia bearing the name "Emil Grundza" and birth date of "September 15, 1990." This identification was later confirmed to be fictitious based on fingerprint identification of CHIMIREL by Immigration

and Customs Enforcement ("ICE") and by CHIMIREL's own admission during a consensual interview with law enforcement.

47. ICE further confirmed that CHIMIREL had no lawful presence in the United States. CHIMIREL later confirmed to law enforcement during a consensual interview that he was illegally in the United States and had entered via the southern border into Texas.

48. Based on my review of law enforcement database records, CHIMIREL had a criminal history dating back to 2018 in the United States. CHIMIREL's criminal history in the United States included charges for immigration violations, theft, receiving stolen goods, and credit card fraud, among other criminal violations.

49. When asked to identify himself, ORBULETU provided the name "Petrisor ORBULETU." ORBULETU did not provide an identification card when requested by law enforcement, but law enforcement databases revealed a Romanian identification card matching the name provided by ORBULETU and bearing the birth date February 2, 1968.

50. ICE further confirmed that ORBULETU had no lawful presence in the United States. ORBULETU later confirmed in a consensual interview to law enforcement that he was illegally in the United States and had entered via the Canadian border.

51. Basde on my review of law enforcement database records, ORBULETU had no known criminal history in the United States.

52. Based on my training and experience, I know that criminals conducting access device fraud schemes will often conceal their true identities by obtaining fictitious IDs to entry the country illegally while evading law enforcement.

53. SUBJECT DEVICE 1 was retrieved from CHIMIREL's pockets and SUBJECT DEVICE 2 was retrieved from ORBULETU's pockets prior to arrest.

54. CHIMIREL and ORBULETU were arrested, read their Miranda warning, and chose initially to speak with law enforcement.

55. During CHIMIREL's consensual interview, he made the following statements, among others, in sum and substance:

a. CHIMIREL entered the United States illegally through Mexico over the southern border into Texas.

b. CHIMIREL is a Romanian citizen from Craiova, Romania.

c. CHIMIREL acknowledged the Slovakia identification cards he provided were fictitious and bore his photo.

d. CHIMIREL confirmed that he had rented the SUBJECT VEHICLE and drove the SUBJECT VEHICLE to the Tarzana ATM.

e. CHIMIREL acknowledged the cards he was using to conduct the unauthorized withdrawals were cloned cards bearing stickers with victim PINs and card balances.

f. CHIMIREL acknowledged that the data used to clone the cards was obtained from skimming incidents.

g. CHIMIREL acknowledged that he possessed a storage unit at Public Storage in Winnetka, California.

56. During ORBULETU's consensual interview, he made the following statements, among others, in sum and substance:

a. ORBULETU entered the United States illegally through Canada via the Canadian border.

b. ORBULETU is a Romanian national from Craiova, Romania.

c. ORBULETU traveled to the Tarzana ATM with CHIMIREL.

d. ORBULETU knew that the cards being used to conduct the unauthorized withdrawals by CHIMIREL were illegitimate and what was happening was wrong or illegal.

57. During consensual questioning by law enforcement, ORBULETU decided to invoke his Miranda rights and stop speaking with law enforcement. Law enforcement ceased any questioning of ORBULETU after ORBULETU indicated he would like to speak with a lawyer.

58. Following CHIMIREL's interview, law enforcement confirmed with an employee at the Public Storage facility at 20140 Sherman Way in Winnetka, California that CHIMIREL possessed storage unit 1213. The Public Storage employee stated that CHIMIREL no longer had access to that storage unit because he had stopped paying the fee for the unit a "couple of months ago." The employee stated that, because the unit was scheduled to go to auction, Public Storage had inventoried the unit consistent with Public Storage's policy, and that the inventory revealed a box that contained point-of-sale terminal parts.

Based on my training and experience, I know that point-of-sale terminal parts can be used for card skimming.

V. TRAINING AND EXPERIENCE REGARDING IDENTITY THEFT CRIMES

59. Based on my training and experience and information obtained from other law enforcement officers who investigate identity theft, I know the following:

a. It is common practice for individuals involved in identity theft, bank fraud, and access device fraud crimes to possess and use multiple digital devices at once. Such digital devices are often used to facilitate, conduct, and track fraudulent transactions and identity theft. Suspects often use digital devices to perpetrate their crimes due to the relative anonymity gained by conducting financial transactions electronically or over the internet. They often employ digital devices for the purposes, among others, of: (1) applying online for fraudulent credit cards; (2) obtaining or storing personal identification information for the purpose of establishing or modifying fraudulent bank accounts and/or credit card accounts; (3) using fraudulently obtained bank accounts and/or credit card accounts to make purchases, sometimes of further personal information; (4) keeping records of their crimes; (5) researching personal information, such as social security numbers and dates of birth, for potential identity theft victims; and (6) verifying the status of stolen access devices.

b. Oftentimes identity thieves take pictures of items reflecting their stolen identities, including items

retrieved from stolen mail or mail matter, with their cellphones.

c. It is also common for identity thieves to keep "profiles" of victims on digital devices. Such "profiles" contain the personal identifying information of victims, such as names, Social Security numbers, dates of birth, driver's license or state identification numbers, alien registration numbers, passport numbers, and employer or taxpayer identification numbers. Identity thieves often keep such information in their cars, storage units, and in their digital devices.

d. It is common for identity thieves, and individuals engaged in bank fraud, access device fraud, and identification document fraud to use equipment and software to print credit and identification cards, to create magnetic strips for credit cards, to use embossing machines to create credit cards, to use laser printers to create checks, and to use magnetic card readers to read and re-encode credit cards. These types of devices are routinely kept where the person will have easy access to such devices, such as on their person or in their cars or homes or storage units. Software relevant to such schemes can also often be found on digital devices, such as computers.

e. Based on my training and experience, I know that individuals who participate in identity theft, bank fraud, and access device fraud schemes often have co-conspirators, and often maintain telephone numbers, email addresses, and other contact information and communications involving their co-

conspirators in order to conduct their business. Oftentimes, they do so on their digital devices. Suspects often use their digital devices to communicate with co-conspirators by phone, text, email, and social media, including sending photos.

Suspects may also have paper copies of such records, which they may keep on their person or in their cars, homes, or storage units.

f. Individuals engaged in mail and identity theft often use multiple digital devices, which they may keep on their person or in their cars.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES²

60. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur

² As used herein, the term "digital device" includes the SUBJECT DEVICES as well as any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain

"booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

61. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

62. The search warrant requests authorization to use the biometric unlock features of a device, based on the following,

which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress 's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of CHIMIREL and

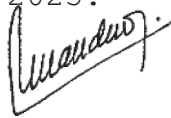
ORBULETU's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

63. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII. CONCLUSION

64. For all of the reasons described above, there is probable cause to believe that CHIMIREL and ORBULETU have committed a violation of 18 U.S.C. § 1029 (a) (2) (use of unauthorized access devices). There is also probable cause that the items to be seized described in Attachment B will be found in a search of the SUBJECT DEVICES as described in Attachment A-1, in the SUBJECT VEHICLE as described in Attachment A-2, and in the public storage unit as described in Attachment A-3.

Attested to by the applicant in
accordance with the requirements
of Fed. R. Crim. P. 4.1 by
telephone on this 3 day of
February, 2023.



THE HONORABLE ~~KAREN L. STEVENSON~~ MARIA A. AUDERO
UNITED STATES MAGISTRATE JUDGE